Alerta de seguridad cibernética	9VSA23-00927-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
TLP	Blanco
Fecha de lanzamiento original	30 de octubre de 2023
Última revisión	30 de octubre de 2023

NOTIFICACIÓN: La información consignada en el presente informe es producto del análisis de múltiples fuentes, de terceras partes, del propio fabricante e investigación propia del CSIRT de Gobierno. La información contenida en los informes o comunicados está afecta a actualizaciones.

Resumen

El CSIRT de Gobierno comparte información de una nueva vulnerabilidad crítica de seguridad que impacta a BIG-IP.

Vulnerabilidades

CVE-2023-46747

Impacto

Vulnerabilidades de riesgo crítico

CVE-2023-46747: Vulnerabilidad que permite que un atacante no autenticado con acceso de red al sistema BIG-IP a través del puerto de administración y/o self IP addresses para ejecutar comandos arbitrarios de sistema. CVSS: 9.8.

Mitigación

Instalar las respectivas actualizaciones entregadas por el proveedor cuando estén disponibles.

Productos afectados

BIG-IP 17.1.0 (Fixed in 17.1.0.3 + Hotfix-BIGIP-17.1.0.3.0.75.4-ENG)
BIG-IP 16.1.0 - 16.1.4 (Fixed in 16.1.4.1 + Hotfix-BIGIP-16.1.4.1.0.50.5-ENG)
BIG-IP 15.1.0 - 15.1.10 (Fixed in 15.1.10.2 + Hotfix-BIGIP-15.1.10.2.0.44.2-ENG)
BIG-IP 14.1.0 - 14.1.5 (Fixed in 14.1.5.6 + Hotfix-BIGIP-14.1.5.6.0.10.6-ENG)
BIG-IP 13.1.0 - 13.1.5 (Fixed in 13.1.5.1 + Hotfix-BIGIP-13.1.5.1.0.20.2-ENG).

Enlaces

https://my.f5.com/manage/s/article/K000137353
https://www.praetorian.com/blog/refresh-compromising-f5-big-ip-with-request-smuggling-cve-2023-46747/
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-46747

CSIRT Gobierno de Chile
Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2023.10.30 12:56:10 -03'00'